

The quantum capacity with symmetric side channels

Graeme Smith, John A. Smolin and Andreas Winter

Abstract—We present an upper bound for the quantum channel capacity that is both additive and convex. Our bound can be interpreted as the capacity of a channel for high-fidelity quantum communication when assisted by a family of channels that have no capacity on their own. This family of assistance channels, which we call symmetric side channels, consists of all channels mapping symmetrically to their output and environment. The bound seems to be quite tight, and for degradable quantum channels it coincides with the unassisted channel capacity. Using this symmetric side channel capacity, we find new upper bounds on the capacity of the depolarizing channel. We also briefly indicate an analogous notion for distilling entanglement using the same class of (one-way) channels, yielding one of the few entanglement measures that is monotonic under local operations with one-way classical communication (1-LOCC), but not under the more general class of local operations with classical communication (LOCC).

Index Terms—entanglement, quantum communication, quantum channel capacity, entanglement, quantum communication, quantum channel capacity

I. INTRODUCTION

The archetypical problem in information theory is finding the capacity of a noisy channel to transmit messages with high fidelity. Already in [1], Shannon provided a simple formula for the capacity of a discrete memoryless channel, with single-letter capacity formulas of more general channels to follow later (see e.g. [2]).

The status of the quantum channel capacity question is not nearly as nice. While there has recently been significant progress towards finding the quantum capacity of a quantum channel [3], [4], [5], the resulting expressions cannot be evaluated in any tractable way, with the exception of some very special channels (e.g., the capacity of the amplitude-damping [6], dephasing [7] and erasure [8] channels are known, most others are not). In fact, there are several capacities that can be defined for a quantum channel, depending on what type of information is to be sent (e.g., quantum or classical) and what sort of resources are allowed to accomplish transmission (e.g., free entanglement, two-way classical communication, etc.). So far only two of these capacities seem to admit single-letter formulas: the entanglement-assisted capacity [9], [10] and the

environment-assisted quantum capacity [11], [12]. The multi-letter formulas available for the other capacities, including the quantum capacity, provide, at best, partial characterizations.

For instance, it was shown in [13], [3], [4], [5] that the capacity for noiseless quantum communication of a quantum channel \mathcal{N} is given by

$$Q(\mathcal{N}) = \lim_{n \rightarrow \infty} \frac{1}{n} \max_{|\phi\rangle_{A(A')^{\otimes n}}} I(A)B^{\otimes n} \omega_{AB^{\otimes n}}. \quad (1)$$

In this expression, \mathcal{N} is a quantum channel mapping quantum states on the vector space A' to states on the space B , and $|\phi\rangle_{A(A')^{\otimes n}}$ is a pure quantum state on n copies of A' together with a reference system A . The state $\omega_{AB^{\otimes n}} = \text{id} \otimes \mathcal{N}^{\otimes n}(|\phi\rangle\langle\phi|_{A(A')^{\otimes n}})$, is the state that results when the n copies of A' are acted on by n copies of the channel \mathcal{N} . Finally, $I(A)B^{\otimes n} \omega_{AB^{\otimes n}} = S(\omega_{B^{\otimes n}}) - S(\omega_{AB^{\otimes n}})$ is known as the *coherent information* [13], which is defined in terms of the von Neumann entropy $S(\rho) = -\text{Tr} \rho \log \rho$. In order to evaluate this regularized formula one would have to perform an optimization over an infinite number of variables, making a numerical approach essentially impossible. Furthermore, it is known that the limit on the right is in general strictly larger than the corresponding single-letter expression [14], [15], [16]: there are channels, \mathcal{N} , for which

$$Q^{(1)}(\mathcal{N}) := \max_{|\phi\rangle_{AA'}} I(A)B \omega_{AB} < Q(\mathcal{N}). \quad (2)$$

In the absence of an explicit formula for the quantum capacity, it is desirable to find upper and lower bounds for Eq. (1). Unfortunately, most known bounds are as difficult to evaluate in general as Eq. (1). Examples of upper bounds that *can* be easily evaluated, at least in some special cases, are given by the no-cloning based arguments of [17], [18], the semi-definite programming bounds of Rains [7], [19] and the closely related relative entropy of entanglement [20]. None of these is expected to be particularly tight—the last two are also upper bounds for the capacity assisted by two-way classical communication (which can be much larger than one-way), whereas the first is based solely on reasoning about where the channel's capacity must be zero. As such, it would be useful to find new upper bounds for the quantum capacity that are both free of regularization and fundamentally one-way. In the following we present just such a bound.

Inspired by the fact that allowing free forward classical communication does not increase the quantum channel capacity [21], we will consider the capacity of a quantum channel assisted by the use of a quantum channel that maps symmetrically to the receiver (Bob) and the environment (Eve). Such assistance channels, which we call *symmetric side channels*, can be used for forward classical communication but are apparently somewhat stronger. They can, however,

Graeme Smith was at the Institute for Quantum Information, Caltech 107–81, Pasadena, CA 91125, USA, and is currently at the IBM T.J. Watson Research Center, Yorktown Heights, NY 10598, USA.

John A. Smolin is at the IBM T.J. Watson Research Center, Yorktown Heights, NY 10598, USA

Andreas Winter is at the Department of Mathematics, University of Bristol, Bristol BS8 1TW, United Kingdom

Graeme Smith received financial support from the US NSF (project PHY-0456720), and NSERC of Canada. John Smolin acknowledges the support of ARO contract DAAD19-01-C-0056. Andreas Winter received support from the U.K. EPSRC via “QIP IRC” and the European Commission under project “QAP” (contract IST-2005-15848), as well as a University of Bristol Research Fellowship.

immediately be seen to have zero quantum capacity, so that while the assisted capacity we find may in general be larger than the usual quantum capacity, one expects that it will provide a fairly tight upper bound. In particular, the *symmetric side channel capacity* (ss-capacity) we find will not be an upper bound for the capacity assisted by two-way classical communication.

The expression we find for the assisted capacity, which we'll call Q_{ss} , turns out to be much easier to deal with than Eq. (1) and has several nice properties. Most importantly, our expression is free of the regularization present in so many quantum capacity formulas. We will also see that Q_{ss} is convex, additive, and that it is equal to Q for the family of degradable channels [22]. We will use these properties to find upper bounds on Q_{ss} of the depolarizing channel which, in turn, will give a significant improvement over known bounds for its unassisted capacity.

It should be emphasized that we have not found an upper bound on the dimension of the side channel needed to attain the assisted capacity, which in general prevents us from evaluating Q_{ss} explicitly or even numerically. While we cannot rule out such a bound, the arguments we use to establish several of Q_{ss} 's nice properties rely explicitly on the availability of an unbounded dimension. This suggests that dealing with an assistance channel of unbounded dimension may be the price we pay for such desirable properties as additivity and convexity, which is reminiscent of the findings of [23], [24].

II. PRELIMINARIES

In this section, we collect the definitions of important concepts and quantities, as well as describing some of their properties.

We will mainly be concerned with finite-dimensional quantum systems. The state of a d dimensional system is described by a *density operator* (or *density matrix*), which is a trace one linear operator on the complex vector space \mathbb{C}^d , typically denoted $\rho \in \mathcal{B}(\mathbb{C}^d)$, where we have used the notation $\mathcal{B}(\mathcal{H})$ to denote the set of bounded linear operators on a space \mathcal{H} . Such a ρ is required to be hermitian, meaning that $\rho = \rho^\dagger$ where the hermitian conjugate \dagger consists of transposition followed by complex conjugation, and positive semidefinite, meaning $\rho \geq 0$. Any such ρ has a spectral decomposition, $\rho = \sum_{i=1}^d \lambda_i |\phi_i\rangle\langle\phi_i|$, where $|\phi_i\rangle\langle\phi_i|$ denotes the projector onto an element $|\phi_i\rangle \in \mathbb{C}^d$, the $|\phi_i\rangle$ satisfy $\langle\phi_j|\phi_i\rangle = \delta_{ij}$, and the λ_i s are nonnegative and sum to one. A rank one density operator, $\rho = |\phi\rangle\langle\phi|$, is called a pure state. We will often include the pure state and density operator's spaces as subscripts, for example ρ_A denotes a density operator on A and $|\phi\rangle_A \in A$.

A useful operation on the set of quantum states is the partial trace. We first define the usual trace of a density operator $\rho = \sum_i \lambda_i |\phi_i\rangle\langle\phi_i|$ to be $\text{Tr } \rho = \sum_i \lambda_i$. If ρ_{AB} is a density operator on the tensor product of A and B , $A \otimes B$, we define the partial trace over B , denoted Tr_B as the unique linear operation satisfying

$$\text{Tr}(|\psi\rangle\langle\psi|(\text{Tr}_B \rho_{AB})) = \text{Tr}((|\psi\rangle\langle\psi| \otimes \mathbb{I}_B)\rho_{AB}) \quad (3)$$

for all $|\psi\rangle \in A$, and where we have let \mathbb{I}_B be the identity on B . Physically, the partial trace over B may be thought of as discarding the B system. The resulting state on A is referred to as the reduced state on A . Given an state ρ_{AB} , we will often use subscripts to denote a reduced state, for example $\rho_A = \text{Tr}_B \rho_{AB}$. We will often be concerned with quantum states on the tensor product of many copies of the same space, where

we will use the notation $A^{\otimes n} = \overbrace{A \otimes \dots \otimes A}^{n \text{ times}}$, and occasionally $A^n = A^{\otimes n}$.

Given two states, ρ and σ , a natural measure of their similarity is the fidelity,

$$F(\rho, \sigma) = \text{Tr} \sqrt{\sqrt{\sigma} \rho \sqrt{\sigma}}, \quad (4)$$

which is equal to 1 if the states are identical and 0 if they are orthogonal. Another useful measure of their similarity is the trace distance, defined as

$$D(\rho, \sigma) = \frac{1}{2} \text{Tr} |\rho - \sigma|, \quad (5)$$

where $|A| = \sqrt{A^\dagger A}$. These two measures are related [25] according to

$$1 - F(\rho, \sigma) \leq D(\rho, \sigma) \leq \sqrt{1 - F(\rho, \sigma)^2}. \quad (6)$$

The physical operations that can be applied a quantum state are *completely positive trace preserving* (CPTP) linear maps from $\mathcal{B}(\mathcal{H}_1)$ to $\mathcal{B}(\mathcal{H}_2)$, where \mathcal{H}_1 and \mathcal{H}_2 are the input and output spaces, respectively. A positive linear map, \mathcal{N} , satisfies the requirement $\mathcal{N}(\rho) \geq 0$ for every $\rho \geq 0$. In addition, a linear map with input space \mathcal{H}_1 and output space \mathcal{H}_2 can be extended to a map from $\mathcal{H}_3 \otimes \mathcal{H}_1$ to $\mathcal{H}_3 \otimes \mathcal{H}_2$, where \otimes denotes a tensor product of the spaces, by choosing the extended map to act as the identity on \mathcal{H}_3 . If the extended map, which we will denote $\text{id}_{\mathcal{H}_3} \otimes \mathcal{N}$, is positive for any choice of \mathcal{H}_3 , the map \mathcal{N} is called *completely positive*. Together with the trace-preserving requirement, demanding complete positivity ensures that CPTP maps are the most general class of linear operations mapping density operators to density operators. Due to the Stinespring dilation theorem [26], a CPTP map (or *quantum channel*) \mathcal{N} , with input space A and output space B can always be represented as an isometric embedding of A into $B \otimes E$ for some environment space E , followed by a partial trace over E . In other words, there will be an isometry $U : A \rightarrow B \otimes E$, satisfying $U^\dagger U = \text{id}_A$, such that $\mathcal{N}(\rho) = \text{Tr}_E U \rho U^\dagger$. Sometimes the isometry corresponding to a channel \mathcal{N} will be called $U_{\mathcal{N}}$. This dilation, of which we shall make free use, is unique up to unitary equivalences of E .

There is another representation of a quantum channel is in terms of its Kraus decomposition. Any quantum channel with input space A and output space B can be expressed as

$$\mathcal{N}(\rho) = \sum_k A_k \rho A_k^\dagger, \quad (7)$$

where A_k are linear maps from A to B with $\sum_k A_k^\dagger A_k = \mathbb{I}_A$, and \mathbb{I}_B is the identity on B . In contrast to \mathbb{I}_B , which is an operator on the vector space B , we denote the identity channel

on $\mathcal{B}(B)$ as id_B , which acts according to $\text{id}_B(\rho) = \rho$ for all $\rho \in \mathcal{B}(B)$.

A channel of particular interest is the depolarizing channel, which maps a two-dimensional space (or, *qubit*) to a two-dimensional space. This channel is the quantum analogue of the binary symmetric channel. For any qubit density operator, $\rho \in \mathcal{B}(\mathbb{C}^2)$, the depolarizing channel with error probability p acts as

$$\mathcal{N}_p(\rho) = (1-p)\rho + \frac{p}{3}X\rho X + \frac{p}{3}Y\rho Y + \frac{p}{3}Z\rho Z, \quad (8)$$

where X , Y , and Z are the Pauli matrices,

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad (9)$$

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad (10)$$

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \quad (11)$$

Even the capacity of this relatively simple quantum channel is unknown. In Section IV we will find upper bounds on this capacity.

The von Neumann entropy of a density operator ρ on a space A is given by $S(\rho) = -\text{Tr} \rho \log \rho$. We will often use the notation $S(A)_\rho$ to denote the entropy of a state ρ on a space A and, when it is clear to which state we refer, we will also simply write $S(A)$. The *coherent information of A given B* of a bipartite state $\rho_{AB} \in \mathcal{B}(A \otimes B)$ is defined as

$$I(A|B)_{\rho_{AB}} = S(\rho_B) - S(\rho_{AB}), \quad (12)$$

or equivalently, $I(A|B)_{\rho_{AB}} = S(B)_{\rho_B} - S(AB)_{\rho_{AB}}$. As with the entropy, when there is no ambiguity as to which state is being discussed, we will simply write $I(A|B) = S(A) - S(AB)$. The coherent information satisfies a quantum data-processing inequality with respect to processing on the B system, meaning that for any state ρ_{AB} and channel, \mathcal{N} , mapping B to C ,

$$I(A|B)_{\rho_{AB}} \geq I(A|C)_{\text{id}_A \otimes \mathcal{N}(\rho_{AB})}. \quad (13)$$

This data processing inequality is a simple consequence of the strong subadditivity of von Neumann entropy [27], and was first pointed out by [13]. The failure of the analogous data processing inequality on the A system [28], [15] is closely related to the need for a regularization in the formula for the quantum channel capacity in Eq. (1).

A useful property of the von Neumann entropy is that is continuous—two states which are close in terms of trace distance have entropies which are correspondingly close. More specifically, Fannes has shown [29] that if ρ and σ are states on a d -dimensional space with trace distance $D(\rho, \sigma) \leq 1/e$, then

$$|S(\rho) - S(\sigma)| \leq D(\rho, \sigma) \log d - D(\rho, \sigma) \log(D(\rho, \sigma)). \quad (14)$$

If we do not require $D(\rho, \sigma) \leq 1/e$, we have a slightly looser bound of

$$|S(\rho) - S(\sigma)| \leq D(\rho, \sigma) \log d + \frac{\log e}{e}. \quad (15)$$

In light of the relationship between fidelity and trace distance expressed in Eq. (6), we also have the relation

$$|S(\rho) - S(\sigma)| \leq \sqrt{1 - F(\rho, \sigma)} \log d + \frac{\log e}{e}, \quad (16)$$

which we will find useful in proving the converse of our coding theorem below.

Finally, we will occasionally use the *quantum mutual information*,

$$I(A; B)_{\rho_{AB}} = S(A)_{\rho_A} + S(B)_{\rho_B} - S(AB)_{\rho_{AB}}, \quad (17)$$

which derives an operational meaning from its role in the single-letter formula for the entanglement assisted capacity [9].

III. DEFINITIONS AND PROPERTIES OF CAPACITIES

A. Unassisted Quantum Capacity

Before studying the symmetric side channel assisted capacity, we first review the usual, unassisted, quantum capacity problem. In this scenario, illustrated in Fig. 1, our sender and receiver are given access to asymptotically many uses of a quantum channel: $\mathcal{N}^{\otimes n}$. If the input space of \mathcal{N} is A and the output space B , our goal is to find a subspace $C \subset A^{\otimes n}$ and a decoding operation $\mathcal{D}_n : \mathcal{B}(B^{\otimes n}) \rightarrow \mathcal{B}(C)$ such that every state $|\psi\rangle \in C$ can be decoded with high fidelity after it is sent through the channel:

$$\mathcal{D}_n \circ \mathcal{N}^{\otimes n}(|\psi\rangle\langle\psi|) \approx |\psi\rangle\langle\psi|. \quad (18)$$

Of course, our goal is to find the largest possible code C .

More formally, we say a rate R is achievable if for every $\epsilon > 0$ and sufficiently large n , there is a code $C_n \subset A^{\otimes n}$ with $\log \dim C_n \geq Rn$ and a decoding operation $\mathcal{D}_n : \mathcal{B}(B^{\otimes n}) \rightarrow \mathcal{B}(C_n)$ such that for all $|\psi\rangle \in C_n$, the fidelity

$$F(|\psi\rangle\langle\psi|, \mathcal{D}_n \circ \mathcal{N}^{\otimes n}(|\psi\rangle\langle\psi|)) \geq 1 - \epsilon. \quad (19)$$

The *capacity* of \mathcal{N} is defined to be the largest such achievable rate.

The best known strategy for generating good quantum codes is based on a random coding argument [4], [5]. Given a channel \mathcal{N} mapping A' to B and a state $|\phi\rangle_{AA'}$, the reduced state $\phi_{A'} = \text{Tr}_A |\phi\rangle\langle\phi|_{AA'}$ provides a prescription for generating good codes with rates up to the coherent information,

$$R = I(A|B)_{(\mathbb{I}_A \otimes \mathcal{N})(|\phi\rangle\langle\phi|_{AA'})}. \quad (20)$$

If one chooses the basis of a blocklength n code by selecting random vectors that are, roughly speaking, distributed like $\phi_{A'}^{\otimes n}$, as long as the rate of the code is no more than this coherent information, it will with high probability allow high fidelity transmission.

As it turns out, when one evaluates the coherent information that can be generated with m uses of a channel, it will in some cases exceed m times the maximum coherent information that can be generated with one copy. This means that by using codes that are not chosen to resemble some i.i.d. input state, but rather whose distribution is correlated across several copies of the channel, it is possible to find better codes. All known examples of this effect occur in channels for which the single-letter coherent information is either zero or very small, where

it seems to be rather generic. While some progress was made in [16], there is still no systematic understanding of how to generate non-i.i.d. high performance codes.

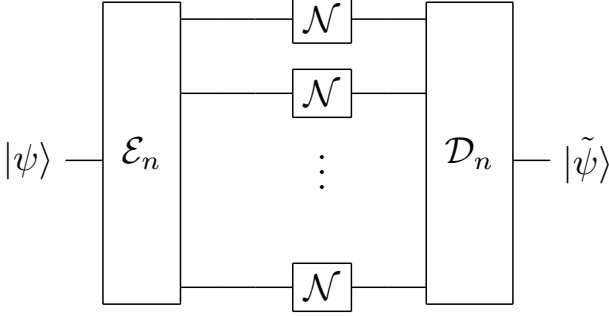


Fig. 1. The unassisted quantum capacity problem. Given n uses of a quantum channel, $\mathcal{N} : \mathcal{B}(A') \rightarrow \mathcal{B}(B)$ we would like to find a quantum code $C_n \subset (A')^{\otimes n}$ such that every $|\psi\rangle \in C_n$ can be decoded with high fidelity after being sent through $\mathcal{N}^{\otimes n}$. The rate of C_n is defined as $R = \frac{1}{n} \log \dim C_n$, and the optimal such rate is called the quantum capacity. The best known expression for the quantum capacity is the multi-letter formula in Eq. (1).

B. Symmetric Side Channel Assisted Capacity

We now turn to our assisted quantum capacity problem. First let $W_d \subset \mathbb{T} \otimes \perp$ be the $d(d+1)/2$ -dimensional symmetric subspace between d -dimensional spaces \mathbb{T} and \perp . W_d is spanned by the following basis labeled by $i, j \in \{1, \dots, d\}$ with $i \leq j$:

$$\begin{aligned} |(i, j)\rangle &= \frac{1}{\sqrt{2}} (|i\rangle|j\rangle + |j\rangle|i\rangle) \quad \text{for } i \neq j \\ &= |i\rangle|i\rangle \quad \text{for } i = j. \end{aligned} \quad (21)$$

$$(22)$$

Now, we let $V_d : \mathbb{C}^{d(d+1)/2} \rightarrow W_d$ be an isometry which maps a basis of $\mathbb{C}^{d(d+1)/2}$ to these $|(i, j)\rangle$ in some order. The d -dimensional symmetric side channel is defined to be the channel mapping $\mathcal{B}(\mathbb{C}^{d(d+1)/2})$ to $\mathcal{B}(\mathbb{T})$ that is obtained by applying V_d followed by the partial trace over \perp :

$$\mathcal{A}_d(\rho) = \text{Tr}_{\perp} V_d \rho V_d^\dagger. \quad (23)$$

Because \mathcal{A}_d maps symmetrically between its output (\mathbb{T}) and environment (\perp), its quantum capacity will turn out to be zero. As a result, one would expect that allowing \mathcal{A}_d as a free resource to be used along with some channel \mathcal{N} , the resulting assisted capacity would provide a reasonably tight upper bound for the unassisted capacity of \mathcal{N} . Furthermore, when we define such an assisted capacity, we will find that it is much better behaved than the unassisted capacity seems to be.

Formally, for a channel $\mathcal{N} : \mathcal{B}(\tilde{A}) \rightarrow \mathcal{B}(B)$, we say that a rate R is *ss-achievable* if for all $\epsilon > 0$ and sufficiently large n , there is a dimension d_n , a code $C_n \subset \tilde{A}^{\otimes n} \otimes W_{d_n}$ with $\log \dim C_n \geq Rn$, and a decoding operation $\mathcal{D}_n : \mathcal{B}(B^{\otimes n} \otimes \mathbb{C}^{d_n})$ such that for all states $|\psi\rangle \in C_n$, the reconstructed state $\mathcal{D}_n[(\mathcal{N}^{\otimes n} \otimes \mathcal{A}_{d_n})|\psi\rangle\langle\psi|]$ has a fidelity of at least $1 - \epsilon$ with the original state $|\psi\rangle\langle\psi|$. The *ss-capacity*, which we will denote by $Q_{\text{ss}}(\mathcal{N})$, is defined as the supremum of all ss-achievable rates.

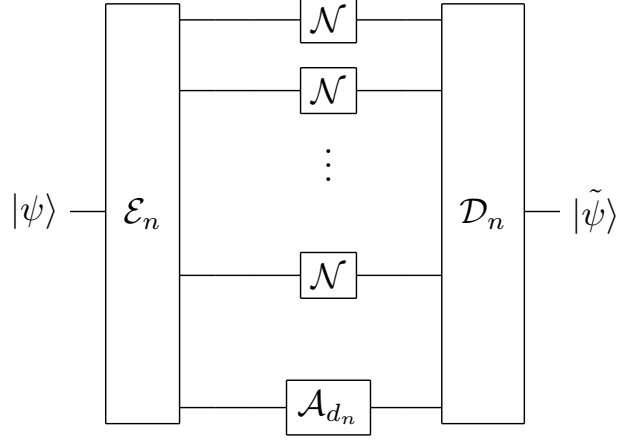


Fig. 2. The quantum capacity with symmetric assistance. Given n uses of a quantum channel, $\mathcal{N} : \mathcal{B}(A') \rightarrow \mathcal{B}(B)$, we also now have free access to a zero-capacity symmetric side channel with arbitrary output dimension, $\mathcal{A}_{d_n} : \mathcal{B}(\mathbb{C}^{d_n(d_n+1)/2}) \rightarrow \mathcal{B}(\mathbb{C}^{d_n})$. Our goal is to find the highest rate subspace of the input spaces $(A')^{\otimes n} \otimes \mathbb{C}^{d_n(d_n+1)/2}$ that still allows high-fidelity reconstruction of every state in the space after the channels have been applied. The best known expression for the capacity in this setting is the single-letter formula of Eq. (27).

Note that assistance by the symmetric channels includes free use of classical communication, as the dephasing operation $|x\rangle \rightarrow |x\rangle|x\rangle$ is obtained by restricting \mathcal{A}_d to a subspace.

We are now in a position to introduce a quantity that will play a central role in our study of the ss-capacity. Letting $\mathcal{N} : \mathcal{B}(\tilde{A}) \rightarrow \mathcal{B}(B)$ be a channel, we define $Q_{\text{ss}}^{(1)}(\mathcal{N})$ to be the supremum over all states $|\phi\rangle\langle\phi|_{A\tilde{A}\mathbb{T}\perp}$ that are invariant under the permutation of \mathbb{T} and \perp , of the coherent information of A given $B\mathbb{T}$, evaluated after the \tilde{A} register of ϕ is acted on by \mathcal{N} . That is, we let

$$\omega_{AB\mathbb{T}\perp} = (\text{id}_{A\mathbb{T}\perp} \otimes \mathcal{N})\phi_{A\tilde{A}\mathbb{T}\perp}, \quad (24)$$

$$Q_{\text{ss}}^{(1)}(\mathcal{N}) = \sup_{\phi_{A\tilde{A}\mathbb{T}\perp}} I(A)B\mathbb{T}\omega = \sup_d Q^{(1)}(\mathcal{N} \otimes \mathcal{A}_d), \quad (25)$$

where the supremum is over all pure states $\phi_{A\tilde{A}\mathbb{T}\perp}$ invariant under the swap $\mathbb{T} \leftrightarrow \perp$ of \mathbb{T} and \perp . The rightmost, alternative, expression for $Q_{\text{ss}}^{(1)}(\mathcal{N})$ is seen as follows. On the one hand, for every state $|\phi\rangle \in A\tilde{A}W_d$, $(\mathbb{I}_{A\tilde{A}} \otimes V_d)|\phi\rangle$ is a state on $A\tilde{A}\mathbb{T}\perp$ that is symmetric in $\mathbb{T}\perp$, so that the coherent information of $(\text{id} \otimes \mathcal{N} \otimes \mathcal{A}_d)\phi_{A\tilde{A}W_d}$ is exactly $I(A)B\mathbb{T}$. On the other hand, if we have a pure state $\phi_{A\tilde{A}\mathbb{T}\perp}$ that is invariant under the exchange of \mathbb{T} and \perp , it must be an eigenvector of the swap operator with eigenvalue 1 or -1 . In the latter case we can extend \mathbb{T} and \perp with a qubit and tensor a singlet onto $|\phi\rangle$ —this doesn't change the coherent information but results in a vector $|\phi\rangle$ which is invariant under swapping \mathbb{T} and \perp . As a result, $\text{Tr}_{A\tilde{A}} \phi$ is supported on the symmetric subspace of $\mathbb{T}\perp$ and we can present $|\phi\rangle$ as the image of a pure state under some $\mathbb{I}_{A\tilde{A}} \otimes V_d$.

For later use, we start by deriving a different formula for $Q_{\text{ss}}^{(1)}$.

Lemma 1 For any channel \mathcal{N} with Stinespring dilation $U_{\mathcal{N}} :$

$$A \rightarrow BE,$$

$$Q_{\text{ss}}^{(1)}(\mathcal{N}) = \sup_{\rho_{A\tilde{A}F}} \frac{1}{2} [I(A)BF]_{\omega} - I(A)EF]_{\omega}, \quad (26)$$

with respect to the state $\omega_{ABEF} = (\mathbb{I}_{AF} \otimes U_{\mathcal{N}}) \rho (\mathbb{I}_{AF} \otimes U_{\mathcal{N}})^{\dagger}$.

Proof: We may think of $\rho_{A\tilde{A}F}$ as the reduced state $\text{Tr}_{F'} \phi_{A\tilde{A}FF'}$ of a pure state $|\phi\rangle$, and look at the information quantities in the lemma w.r.t. the state $(\mathbb{I}_{AFF'} \otimes U_{\mathcal{N}})|\phi\rangle$. Then, it is an elementary identity that $I(A)EF = -I(A)BF'$, and in the r.h.s. of Eq. (26) the expression becomes

$$\frac{1}{2} [I(A)BF + I(A)BF'].$$

Notice that if ϕ is symmetric under swapping F and F' , this is equal to $I(A)BF$.

In general, we can, with $\top = FG$ and $\perp = F'G'$ (where G and G' label qubit registers), define

$$\begin{aligned} |\varphi\rangle_{A\tilde{A}\top\perp} &= \frac{1}{\sqrt{2}} |\phi\rangle_{A\tilde{A}FF'} |01\rangle_{GG'} \\ &+ \frac{1}{\sqrt{2}} (\mathbb{I}_{A\tilde{A}} \otimes \text{SWAP}_{FF'}) |\phi\rangle_{A\tilde{A}FF'} |10\rangle_{GG'}, \end{aligned}$$

where $\text{SWAP}_{FF'}|i\rangle_F|j\rangle_{F'} = |j\rangle_F|i\rangle_{F'}$ is a unitary that permutes F and F' . Then, with respect to the state $\Omega_{AB\top\perp} = (\text{id}_{A\top\perp} \otimes \mathcal{N})\varphi$,

$$\frac{1}{2} [I(A)BF + I(A)BF']_{\omega} = I(A)B\top]_{\Omega},$$

and we are done. \blacksquare

It will turn out that $Q_{\text{ss}}^{(1)}(\mathcal{N})$ is exactly the ss-capacity of \mathcal{N} , as the following theorem shows.

Theorem 2 For all channels \mathcal{N} ,

$$Q_{\text{ss}}(\mathcal{N}) = Q_{\text{ss}}^{(1)}(\mathcal{N}) = \sup_{\phi_{A\tilde{A}\top\perp}} I(A)B\top]_{\omega} \quad (27)$$

with $\omega_{AB\top\perp} = (\text{id}_{A\top\perp} \otimes \mathcal{N})\phi_{A\tilde{A}\top\perp}$ and where the optimization is over all $\phi_{A\tilde{A}\top\perp}$ invariant under permuting \top and \perp .

We will prove this with the following two lemmas.

Lemma 3 $Q_{\text{ss}}^{(1)}$ is additive; that is, $Q_{\text{ss}}^{(1)}(\mathcal{N}_1 \otimes \mathcal{N}_2) = Q_{\text{ss}}^{(1)}(\mathcal{N}_1) + Q_{\text{ss}}^{(1)}(\mathcal{N}_2)$ for arbitrary channels \mathcal{N}_1 and \mathcal{N}_2 .

Proof: We use the previous lemma, and observe, for a state $\rho_{A\tilde{A}_1\tilde{A}_2F}$, and

$$\omega_{AB_1E_1B_2E_2F} = (\mathbb{I}_{AF} \otimes U_{\mathcal{N}_1} \otimes U_{\mathcal{N}_2}) \rho (\mathbb{I}_{AF} \otimes U_{\mathcal{N}_1} \otimes U_{\mathcal{N}_2})^{\dagger},$$

the identity (with respect to ω)

$$\begin{aligned} I(A)B_1B_2F - I(A)E_1E_2F &= \\ &= (I(A)B_1B_2F - I(A)E_1B_2F) \\ &+ (I(A)E_1B_2F - I(A)E_1E_2F). \end{aligned} \quad (28)$$

If we introduce new auxiliary systems $F_1 := B_2F$ and $F_2 := E_1F$, the above right hand side becomes

$$(I(A)B_1F_1 - I(A)E_1F_1) + (I(A)B_2F_2 - I(A)E_2F_2),$$

which is evidently upper bounded by $Q_{\text{ss}}^{(1)}(\mathcal{N}_1) + Q_{\text{ss}}^{(1)}(\mathcal{N}_2)$, while the supremum of the left hand side in Eq. (28) is $Q_{\text{ss}}^{(1)}(\mathcal{N}_1 \otimes \mathcal{N}_2)$. This shows $Q_{\text{ss}}^{(1)}(\mathcal{N}_1 \otimes \mathcal{N}_2) \leq Q_{\text{ss}}^{(1)}(\mathcal{N}_1) + Q_{\text{ss}}^{(1)}(\mathcal{N}_2)$.

Furthermore, by restricting the optimization in Eq. (25) to states of the form $\phi_{A_1\tilde{A}_1U_1V_1} \otimes \phi_{A_2\tilde{A}_2U_2V_2}$ we see that $Q_{\text{ss}}^{(1)}(\mathcal{N}_1 \otimes \mathcal{N}_2) \geq Q_{\text{ss}}^{(1)}(\mathcal{N}_1) + Q_{\text{ss}}^{(1)}(\mathcal{N}_2)$. \blacksquare

Lemma 3 is the key to showing that the ss-capacity has a single-letter formula. Because this result is central to our study, we comment briefly on why it works. This lemma says that by using \mathcal{N}_1 and \mathcal{N}_2 together with a symmetric side channel to generate coherent information, one does no better than if one uses each \mathcal{N}_i individually to generate ss-assisted coherent information. Given a joint input state to $\mathcal{N}_1 \otimes \mathcal{N}_2 \otimes \mathcal{A}_d$, Lemmas 1 and 3 give a prescription for generating an input state for $\mathcal{N}_1 \otimes \mathcal{A}_{d_1}$ by symmetrizing the output and environment of \mathcal{N}_2 , and similarly for $\mathcal{N}_2 \otimes \mathcal{A}_{d_2}$. In fact, the sum of the coherent informations obtained in this way is at least as much as the total coherent information generated with the joint state. From this explanation, we see also that it is important to allow a large output dimension for our symmetric side channel.

The other ingredient we need is the following multi-letter expression for the ss-capacity, which follows by standard arguments (see, e.g., [5]).

Lemma 4 The ss-capacity Q_{ss} is given by the regularization of $Q_{\text{ss}}^{(1)}$: for any channel \mathcal{N} ,

$$Q_{\text{ss}}(\mathcal{N}) = \lim_{n \rightarrow \infty} \frac{1}{n} Q_{\text{ss}}^{(1)}(\mathcal{N}^{\otimes n}). \quad (29)$$

Proof: To see that the ss-capacity is no less than the right hand side, note that for any $\phi_{A^n B^n \top \perp}$ symmetric under the interchange of \top and \perp , the rate $\frac{1}{n} I(A^n)B^n \top]$ is achievable by the quantum noisy channel coding theorem applied to the channel $\mathcal{N}^{\otimes n} \otimes \mathcal{A}_{d_{\top}}$ [3], [4], [5].

To prove the converse, fix ϵ , let $C \subset \tilde{A}^{\otimes n} W_{d_{\top}}$ be an (n, ϵ) -code of rate R making use of a symmetric side channel with output dimension d_{\top} and let $|\phi\rangle_{CD}$ be a state that is maximally entangled between the subspace C and a reference system D . Then, with the state $\omega = (\text{id} \otimes \mathcal{N}^{\otimes n} \otimes \mathcal{A}_{d_{\top}})\phi$,

$$\begin{aligned} I(D)B^n \top]_{\omega} &\geq I(D)C]_{(\text{id} \otimes \mathcal{D}_{B^n \top})\omega} \\ &\geq Rn - \frac{2 \log e}{e} - 3 \log(d_C) \sqrt{\epsilon} \end{aligned} \quad (30)$$

$$= Rn - \frac{2 \log e}{e} - 3Rn\sqrt{\epsilon}, \quad (31)$$

where we have made use of Eq. (16) twice. As a result, we find $R \leq (1 - 3\sqrt{\epsilon})^{-1} \left(\frac{1}{n} Q_{\text{ss}}^{(1)}(\mathcal{N}^{\otimes n}) + \frac{2 \log e}{ne} \right)$, which completes the proof. \blacksquare

Lemmas 3 and 4 immediately imply the expression for $Q_{\text{ss}}(\mathcal{N})$ quoted in Theorem 2.

From Theorem 2 we can easily show the following proposition.

Proposition 5 Q_{ss} is a convex function of the channel \mathcal{N} .

Proof: Letting \mathcal{N}_1 and \mathcal{N}_2 be channels and $\omega_i = (\text{id} \otimes \mathcal{N}_i \otimes \mathcal{A}_d)\phi$, the convexity of $I(A)B\top)_{\omega_{AB\top}}$ [27] gives us

$$I(A)B\top)_{p\omega_1 + (1-p)\omega_2} \leq pI(A)B\top)_{\omega_1} + (1-p)I(A)B\top)_{\omega_2},$$

where $p\omega_1 + (1-p)\omega_2 = [\text{id} \otimes (p\mathcal{N}_1 + (1-p)\mathcal{N}_2) \otimes \mathcal{A}_d]\phi$. This implies

$$\begin{aligned} \max_{\phi} I(A)B\top)_{\omega} &\leq p \max_{\phi} I(A)B\top)_{\omega_1} \\ &\quad + (1-p) \max_{\phi} I(A)B\top)_{\omega_2}, \end{aligned}$$

which tells us exactly that $Q_{\text{ss}}(p\mathcal{N}_1 + (1-p)\mathcal{N}_2) \leq pQ_{\text{ss}}(\mathcal{N}_1) + (1-p)Q_{\text{ss}}(\mathcal{N}_2)$. ■

IV. IMPLICATIONS FOR THE UNASSISTED CAPACITY

In this section we explore some of the limitations that the ss-capacity places on the standard capacity of a quantum channel. As noted in the introduction, by simply not using the assistance channel provided, it is possible to communicate over a channel at the unassisted rate. In other words,

$$Q(\mathcal{N}) \leq Q_{\text{ss}}(\mathcal{N}). \quad (32)$$

Furthermore, as we will now see, this upper bound is actually an equality for the class of channels known as *degradable* [22]. As mentioned above, every channel, \mathcal{N} , can be expressed as an isometry $U_{\mathcal{N}} : A \rightarrow BE$ followed by a partial trace, such that $\mathcal{N}(\rho) = \text{Tr}_E U_{\mathcal{N}} \rho U_{\mathcal{N}}^\dagger$. The complementary channel of \mathcal{N} , which we call $\hat{\mathcal{N}}$, is the channel that results by tracing out system B rather than the environment: $\hat{\mathcal{N}}(\rho) = \text{Tr}_B U_{\mathcal{N}} \rho U_{\mathcal{N}}^\dagger$. Since the Stinespring dilation is unique up to isometric equivalence of E , $\hat{\mathcal{N}}$ is well-defined up to isometries on the output. A channel is degradable if there exists a completely positive trace preserving map, $\mathcal{D} : \mathcal{B}(B) \rightarrow \mathcal{B}(E)$, which “degrades” the channel \mathcal{N} to $\hat{\mathcal{N}}$. In other words, $\mathcal{D} \circ \mathcal{N} = \hat{\mathcal{N}}$. The capacity of a degradable channel is given by the single letter maximization of the coherent information, as shown in [22]. Furthermore, we will now show that the ss-capacity of a degradable channel is given by the same formula. That is, the assistance channels we have been considering are of no use at all for a degradable channel.

Theorem 6 *If \mathcal{N} is degradable, then $Q_{\text{ss}}(\mathcal{N}) = Q(\mathcal{N})$.*

Proof: Fix $|\phi\rangle_{A\bar{A}W_d}$. Then, with respect to the state $\omega_{AB\top} = (\text{id}_A \otimes \mathcal{N} \otimes \mathcal{A})\phi$,

$$I(A)B\top) \leq I(A\top)B) + I(ABE)\top) \quad (33)$$

exactly when $I(E; \perp) \leq I(B; \top)$, which is true if \mathcal{N} is degradable by the monotonicity of mutual information under local operations (the monotonicity of quantum mutual information is a special case of the monotonicity of quantum relative entropy, first proved in [30]). This implies that the maximum value of the left hand side of Eq. (33) is no larger than the maximum of the right hand side. The maximum of the first term on the right is exactly the single-shot maximization of the coherent information, $Q^{(1)}(\mathcal{N})$, whereas the maximum of the second is zero (because of the no-cloning argument), so

that $I(A)B\top)_{\omega} \leq Q(\mathcal{N})$. Furthermore, by choosing a trivial assistance channel, the left hand side can attain the right hand side. ■

As an aside, we note that the definition of $Q_{\text{ss}}^{(1)}$ can be reformulated in terms of degradable channels. In particular, we call a channel $\mathcal{A} : \mathcal{B}(A) \rightarrow \mathcal{B}(B)$ with complementary channel $\hat{\mathcal{A}} : \mathcal{B}(A) \rightarrow \mathcal{B}(E)$ *bidegradable* if both \mathcal{A} and $\hat{\mathcal{A}}$ are degradable, which is equivalent to requiring the existence of channels $\mathcal{D} : \mathcal{B}(B) \rightarrow \mathcal{B}(E)$ and $\mathcal{D}' : \mathcal{B}(E) \rightarrow \mathcal{B}(B)$ such that $\mathcal{D} \circ \mathcal{A} = \hat{\mathcal{A}}$ and $\mathcal{D}' \circ \hat{\mathcal{A}} = \mathcal{A}$. Then, using the Stinespring theorem on such \mathcal{A} and the data processing inequality for the coherent information (Eq. (13)), we have

$$Q_{\text{ss}}^{(1)}(\mathcal{N}) = \sup_{\mathcal{A} \text{ bidegradable}} Q^{(1)}(\mathcal{N} \otimes \mathcal{A}).$$

Returning to our goal of finding upper bounds for Q , we will make use of Theorem 6, which allows us to calculate the ss-capacity of any degradable channel. If a channel \mathcal{N} can be written as a convex combination of degradable channels, Theorem 6, together with the convexity of Q_{ss} , provides an upper bound for $Q_{\text{ss}}(\mathcal{N})$ and therefore also $Q(\mathcal{N})$.

For instance, the depolarizing channel can be written as a convex combination of dephasing-type channels,

$$\begin{aligned} \mathcal{N}_p(\rho) &= (1-p)\rho + \frac{p}{3}X\rho X + \frac{p}{3}Y\rho Y + \frac{p}{3}Z\rho Z \\ &= \frac{1}{3}\mathcal{X}_p(\rho) + \frac{1}{3}\mathcal{Y}_p(\rho) + \frac{1}{3}\mathcal{Z}_p(\rho), \end{aligned}$$

where $\mathcal{X}_p(\rho) = (1-p)\rho + pX\rho X$ and similarly for \mathcal{Y}_p and \mathcal{Z}_p . From this we conclude that

$$Q_{\text{ss}}(\mathcal{N}_p) \leq \frac{1}{3}Q_{\text{ss}}(\mathcal{X}_p) + \frac{1}{3}Q_{\text{ss}}(\mathcal{Y}_p) + \frac{1}{3}Q_{\text{ss}}(\mathcal{Z}_p) = 1 - H(p),$$

where we have used the fact that \mathcal{X}_p , \mathcal{Y}_p , and \mathcal{Z}_p are degradable and have ss-capacity $1 - H(p)$ (Theorem 6). This reproduces the upper bounds of [20], [7], [19], which have been the best known for small p .

We can also evaluate $Q_{\text{ss}}(\mathcal{N}_p)$ for $p = \frac{1}{4}$ as follows. For this value of p , there is a CP-map which can be composed with the complementary channel, $\hat{\mathcal{N}}_p$, to generate \mathcal{N}_p [17]. This immediately implies $Q_{\text{ss}}(\mathcal{N}_{1/4}) = 0$, since otherwise both Bob and Eve could both reconstruct the encoded state with high fidelity, giving a violation of the no-cloning theorem. More explicitly, for any state $|\phi\rangle_{A\bar{A}\top\perp}$ with the symmetry $\top \leftrightarrow \perp$ we have, with respect to the state $(\text{id} \otimes \mathcal{N}_{1/4})\phi$,

$$I(A)B\top) = -I(A)E\top) \leq -I(A)B\top), \quad (34)$$

from which we conclude $Q_{\text{ss}}(\mathcal{N}_{1/4}) = 0$, and where the second step is due to the quantum data processing inequality (Eq. (13)). This reproduces the bound of [17], and furthermore, because the ss-capacity is convex, we find that

$$Q(\mathcal{N}_p) \leq Q_{\text{ss}}(\mathcal{N}_p) \leq \text{conv}(1 - H(p), (1 - 4p)_+), \quad (35)$$

with the notation

$$x_+ = \begin{cases} x & \text{if } x \geq 0, \\ 0 & \text{if } x < 0. \end{cases}$$

It is important to note that the quantum capacity Q is not known to be convex and, indeed, may well not be—in the two way scenario, both nonadditivity and nonconvexity would be implied [31] by the conjecture of [32] that a family of Nonpositive Partial Transpose (NPT) Werner states is bound entangled. Thus, while the two bounds above were already known, it was not clear that the convex hull of these was also an upper bound.

We will now provide a tighter bound for $Q_{ss}(\mathcal{N}_p)$, by expressing the depolarizing channel as a convex combination of amplitude-damping channels, which were shown to be degradable in [6]. The amplitude-damping channel can be expressed as

$$\Delta_\gamma(\rho) = A_0 \rho A_0^\dagger + A_1 \rho A_1^\dagger, \quad (36)$$

where

$$A_0 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{pmatrix} \quad \text{and} \quad A_1 = \begin{pmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{pmatrix}. \quad (37)$$

From this we find that

$$\frac{1}{2} \Delta_\gamma(\rho) + \frac{1}{2} Y \Delta_\gamma(Y \rho Y) Y = \mathcal{N}_{(q,q,p_z)}(\rho),$$

where

$\mathcal{N}_{(q,q,p_z)}(\rho) = (1 - 2q - p_z) \rho + qX\rho X + qY\rho Y + p_z Z\rho Z$, with $q = \frac{\gamma}{4}$ and $p_z = \frac{1}{2} (1 - \frac{\gamma}{2} - \sqrt{1-\gamma})$. The depolarizing channel can now be expressed as

$$\mathcal{N}_{2q+p_z} = \frac{1}{3} \mathcal{N}_{(q,q,p_z)} + \frac{1}{3} \mathcal{N}_{(q,p_z,q)} + \frac{1}{3} \mathcal{N}_{(p_z,q,q)}, \quad (38)$$

so that \mathcal{N}_p is a convex combination of amplitude damping channels with $\gamma_p = 4\sqrt{1-p}(1 - \sqrt{1-p})$. This gives us an upper bound, shown in Figure 3, of

$$Q(\mathcal{N}_p) \leq Q_{ss}(\mathcal{N}_p) \leq \text{conv}(Q(\Delta_{\gamma_p}), (1-4p)_+), \quad (39)$$

where $Q(\Delta_{\gamma_p})$ is, according to [6], given by

$$Q(\Delta_{\gamma_p}) = \max_{0 \leq t \leq 1} [H_2(t(1-\gamma_p)) - H_2(t\gamma_p)]. \quad (40)$$

The resulting bound is strictly stronger than the previously known bounds of $1 - H(p)$ and $(1 - 4p)_+$ for all $0.25 > p > 0.04$.

V. A LOWER BOUND FOR Q_{ss}

In this section we present a particular state relative to which the quantity optimized in Eq. (26) to give Q_{ss} is, for the depolarizing channel, strictly larger than the hashing lower bound for Q_{ss} mentioned in the previous section. Letting

$$|\phi\rangle = \sum_{s,t=0}^1 \sqrt{q_{st}} X^s Z^t \otimes \mathbb{I} |\Phi^+\rangle_{AA} |st\rangle_F, \quad (41)$$

we have

$$\begin{aligned} Q_{ss}^{(1)}(\mathcal{N}) &= \sup_{\rho_{A\bar{A}F}} \frac{1}{2} [I(A)BF) - I(A)EF)] \\ &\geq \frac{1}{2} I(A)BF)_{(\text{id}_{A\bar{A}} \otimes \mathcal{N}_p)(\phi)} \\ &\quad + \frac{1}{2} I(A)B)_{(\text{id}_{A\bar{A}} \otimes \mathcal{N}_p)(\phi)} \end{aligned} \quad (42)$$

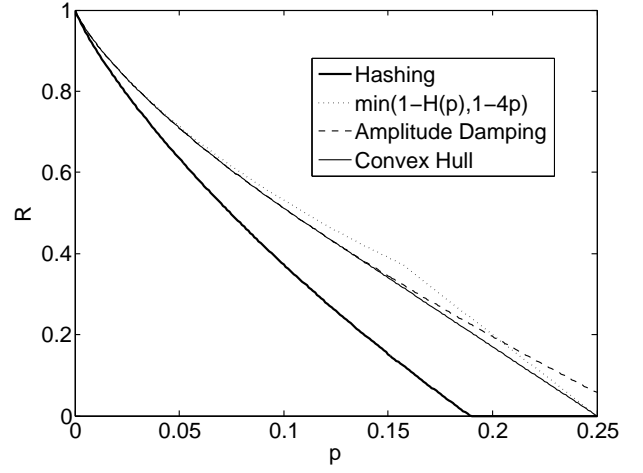


Fig. 3. Our upper bound evaluated for the depolarizing channel: the dotted line is the previous best bound that comes from the minimum of a no-cloning argument and Rains' bound, the dashed line is the capacity of an amplitude damping channel with damping parameter $\gamma_p = 4\sqrt{1-p}(1 - \sqrt{1-p})$; finally, the thin solid line is the convex hull of the first two, our best upper bound on $Q_{ss}(\mathcal{N}_p)$ and $Q(\mathcal{N}_p)$ so far; The thick solid line is the hashing (lower) bound, $1 - H(p) - p \log 3$.

for any choice of q_{st} with $\sum_{st} q_{st} = 1$. For the depolarizing channel, the optimal such q_{st} is of the form

$$q_{st} = (1 - q, q/3, q/3, q/3), \quad (43)$$

which leads to entropies

$$\begin{aligned} S(BF) &= - \left[\frac{1}{2} - \frac{4pq}{9} - 2\eta_{p,q} \right] \log \left[\frac{1}{4} - \frac{2pq}{9} - \eta_{p,q} \right] \\ &\quad - \left[\frac{1}{2} - \frac{4pq}{9} + 2\eta_{p,q} \right] \log \left[\frac{1}{4} - \frac{2pq}{9} + \eta_{p,q} \right] \\ &\quad - \frac{8pq}{9} \log \left[\frac{2pq}{9} \right] \end{aligned} \quad (44)$$

$$\begin{aligned} S(AB) &= - \left[1 - p - q + \frac{4pq}{3} \right] \log \left[1 - p - q + \frac{4pq}{3} \right] \\ &\quad - \left[p + q - \frac{4pq}{3} \right] \log \left[\frac{p+q}{3} - \frac{4pq}{9} \right] \end{aligned} \quad (45)$$

$$\begin{aligned} S(B) &= 1 \\ S(ABF) &= H(p) + p \log 3, \end{aligned}$$

where

$$\eta_{p,q} = \frac{1}{36} \sqrt{81 - 720pq - 512p^2q^2 + 576qp(p+q)}. \quad (46)$$

This gives a lower bound of

$$\begin{aligned} Q_{ss}(\mathcal{N}) &\geq \frac{1}{2} (1 - H(p) - p \log 3) \\ &\quad + \frac{1}{2} (S(BF) - S(AB)), \end{aligned} \quad (47)$$

with $S(BF)$ and $S(AB)$ given by Eqs. (44) and (45), respectively. This, optimized over q , is plotted in Fig. 4. The resulting bound is nonzero up to $p = 0.2124$, which should

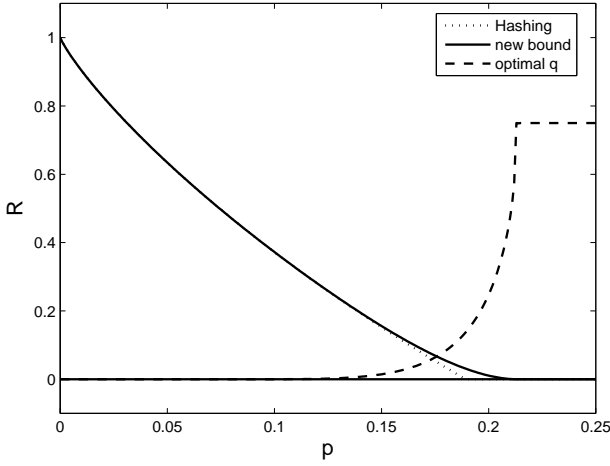


Fig. 4. Our lower bound for the symmetric side channel capacity of the depolarizing channel: The dotted curve is the hashing lower bound for Q_{ss} , which in this case is $1 - H(p) - p \log 3$. The solid curve is Eq (47), evaluated for the optimal value of q . The dashed curve is the optimal value of q .

be compared to the threshold of hashing at $p = 0.1893$ and of the best known codes for the depolarizing channel at 0.19088 [16].

It is intriguing that the form of Eq. (41) corresponds to a preprocessing of \mathcal{N}_p 's input by applying a depolarizing channel whose environment is F , then sending F through the side channel, with the optimal level of preprocessing noise increasing to the completely depolarizing probability of $3/4$ as \mathcal{N}_p 's noise level increases.

VI. ONE-WAY DISTILLATION WITH SYMMETRIC SIDE CHANNELS

Based on the connection between quantum channel capacities and entanglement distillation via local operations with one-way classical communication (1-LOCC) [33], [21], we can define a symmetric side channel assisted distillation notion for bipartite states ρ_{AB} :

$$D_{ss \rightarrow}^{(1)}(\rho) = \sup_{\sigma, \mathcal{E}} I(A') B \tilde{B} (\mathcal{E} \otimes \text{id}_{B \tilde{B}}) \rho \otimes \sigma, \quad (48)$$

where the supremum is over states $\sigma_{\tilde{A} \tilde{B} \tilde{E}}$ (such that $\tilde{B} \simeq \tilde{E}$) with the property $\sigma_{\tilde{A} \tilde{B}} = \sigma_{\tilde{A} \tilde{E}}$ and operations on Alice's system $\mathcal{E} : A \tilde{A} \rightarrow A'$. Observe that these states (or rather their restrictions $\sigma_{\tilde{A} \tilde{B}}$) are often called *two-shareable* or *two-extendable* in the literature. Note also that without loss of generality we may restrict our attention to pure states, at the expense of increasing the dimension of their local supports (which, in any case, is unbounded in the above definition).

For a state ρ_{AB} with purification $|\phi\rangle_{ABE}$ and with respect to the state $\omega_{A'BEF} = (\mathcal{T}_A \otimes \text{id}_{BE})\phi$, with $\mathcal{T} : \mathcal{B}(A) \rightarrow \mathcal{B}(A' \otimes F)$ we have the analogue of Lemma 1:

$$D_{ss \rightarrow}^{(1)}(\rho) = \sup_{\mathcal{T} : A \rightarrow A' F} \frac{1}{2} (I(A')BF) - I(A')EF). \quad (49)$$

Just as for channels, we find that $D_{ss \rightarrow}^{(1)}$ is additive, convex and indeed a 1-LOCC entanglement monotone, reducing to the entropy of entanglement for pure states, and vanishing for all two-shareable states. Furthermore, $D_{ss \rightarrow}^{(1)}(\rho)$ has an operational

meaning—it is the one-way distillable entanglement of ρ when assisted by arbitrary two-shareable states.

The notion of degradability of channels is translated to states as follows: ρ_{AB} is called *degradable* if, for its purification ϕ_{ABE} , there exists a quantum channel $\mathcal{D} : \mathcal{B}(B) \rightarrow \mathcal{B}(E)$ such that $\phi_{AE} = (\text{id}_A \otimes \mathcal{D})\rho_{AB}$. The analogue of the bidegradable channels are states σ_{ABE} such that there are channels degrading both ways, $B \rightarrow E$ and $E \rightarrow B$.

Analogously to our findings for channels, we can prove that $D_{ss \rightarrow}(\rho) = D_{\rightarrow}(\rho)$ for degradable states, so that the upper bounds in the previous section on the quantum capacity of the depolarizing channels, including Fig. 3, translate into upper bounds on the one-way distillable entanglement of two-qubit Werner states.

VII. QUANTUM VALUE ADDED

In Section IV we saw that the ss-capacity of a degradable channel is equal to its unassisted capacity. In fact, we have not been able to show a separation between the ss-capacity and the unassisted capacity for *any* channel. The question arises: Are there \mathcal{N} such that $Q_{ss}(\mathcal{N}) > Q(\mathcal{N})$?

Motivated by this question, for any CPTP map \mathcal{M} , we define the *value added* of \mathcal{M} to be

$$V^{(1)}(\mathcal{M}) := \sup_{\mathcal{N}} [Q^{(1)}(\mathcal{N} \otimes \mathcal{M}) - Q^{(1)}(\mathcal{N})]. \quad (50)$$

In words, $V^{(1)}(\mathcal{M})$ is the largest increase in the optimized coherent information that \mathcal{M} can provide when used as a side channel for some other \mathcal{N} . This definition has the appealing property that $V^{(1)}$ is sub-additive, since

$$\begin{aligned} V^{(1)}(\mathcal{M}_1 \otimes \mathcal{M}_2) &= \sup_{\mathcal{N}} [Q^{(1)}(\mathcal{N} \otimes \mathcal{M}_1 \otimes \mathcal{M}_2) - Q^{(1)}(\mathcal{N})] \\ &\leq \sup_{\mathcal{N}} [Q^{(1)}(\mathcal{N} \otimes \mathcal{M}_1 \otimes \mathcal{M}_2) - Q^{(1)}(\mathcal{N} \otimes \mathcal{M}_2)] \\ &\quad + \sup_{\mathcal{N}} [Q^{(1)}(\mathcal{N} \otimes \mathcal{M}_2) - Q^{(1)}(\mathcal{N})] \\ &\leq V^{(1)}(\mathcal{M}_1) + V^{(1)}(\mathcal{M}_2). \end{aligned}$$

Letting

$$V(\mathcal{M}) := \lim_{n \rightarrow \infty} \frac{1}{n} V^{(1)}(\mathcal{M}^{\otimes n}),$$

we have $V(\mathcal{M}) \leq V^{(1)}(\mathcal{M})$, and furthermore, for all $\epsilon > 0$ and sufficiently large n

$$\begin{aligned} V^{(1)}(\mathcal{M}^{\otimes n}) &= \sup_{\mathcal{N}} [Q^{(1)}(\mathcal{N} \otimes \mathcal{M}^{\otimes n}) - Q^{(1)}(\mathcal{N})] \\ &\geq [Q^{(1)}(\mathcal{M}^{\otimes n} \otimes \mathcal{M}^{\otimes n}) - Q^{(1)}(\mathcal{M}^{\otimes n})] \\ &\geq (2n)(Q(\mathcal{M}) - \epsilon) - nQ(\mathcal{M}), \end{aligned}$$

so that

$$\frac{1}{n} V^{(1)}(\mathcal{M}^{\otimes n}) \geq Q(\mathcal{M}) - 2\epsilon,$$

which gives us $V^{(1)}(\mathcal{M}) \geq V(\mathcal{M}) \geq Q(\mathcal{M})$.

In addition to this upper bound for the capacity, $V^{(1)}$ also provides a sufficient condition for $Q_{ss}(\mathcal{N}) = Q(\mathcal{N})$:

$$\begin{aligned} Q_{ss}(\mathcal{N}) - Q(\mathcal{N}) &= \lim_{n \rightarrow \infty} \frac{1}{n} \left(\sup_d Q^{(1)}(\mathcal{N}^{\otimes n} \otimes \mathcal{A}_d) - Q^{(1)}(\mathcal{N}^{\otimes n}) \right) \\ &\leq \lim_{n \rightarrow \infty} \frac{1}{n} \left(\sup_d \sup_{\mathcal{M}} \left(Q^{(1)}(\mathcal{M} \otimes \mathcal{A}_d) - Q^{(1)}(\mathcal{M}) \right) \right) \\ &\leq \sup_d V^{(1)}(\mathcal{A}_d), \end{aligned}$$

so that $Q_{ss}(\mathcal{N}) = Q(\mathcal{N})$ for all \mathcal{N} as long as $V^{(1)}(\mathcal{A}_d) = 0$ for all d . Unfortunately, although Eq. (50) is nominally single-letter, evaluating $V^{(1)}$ seems to be quite difficult, as it contains an optimization over an infinite number of variables.

VIII. DISCUSSION

We have studied the capacity of a quantum channel given the assistance of an arbitrary symmetric side channel. The capacity formula we find is in many ways more manageable than the known expression for the (unassisted) quantum capacity, and we are able to establish that the ss-capacity is both convex and additive. By taking advantage of the convexity of Q_{ss} and the fact that Q_{ss} and Q coincide for degradable channels, we presented a general method for finding upper bounds to Q and in particular provided a bound for the capacity of the depolarizing channel that is stronger than any previously known result.

We have left many questions unanswered. The most pressing is whether it is possible to bound the dimension of the symmetric side channel needed to achieve the ss-capacity. Such a bound would allow us to evaluate $Q_{ss}(\mathcal{N})$ efficiently, which we expect would provide very tight bounds on Q in many cases.

So far, we have not been able to find a channel for which the ss-capacity and capacity differ. We expect that such channels exist, and a better understanding of when the two capacities differ may point towards simplifications of the quantum capacity formula in Eq. (1).

It is worth mentioning that we first discovered the unsymmetrized version of the quantity $Q_{ss}^{(1)}$ given in Lemma 1, and that it is an upper bound for Q . This was motivated by the quest to find the entanglement analogue of the upper bound on distillable key presented in [34], [35]. It was only later that it became clear that the formula could be made symmetric and interpreted as the quantum capacity of a channel given the family of assistance channels we have considered.

Finally, it should be noted that the approach we have taken here is qualitatively similar to the work of [20], [7], [19] in the two-way scenario. In that work, it was found that *enlarging* the set of operations allowed for entanglement distillation from LOCC to the easier-to-deal-with set of separable or positive-partial-transpose-(PPT)-preserving operations made it possible to establish tighter bounds on two-way distillable entanglement than was possible by considering LOCC protocols directly. Similarly, we have shown that by augmenting a channel with a zero capacity side channel, a simplified capacity formula can

be found that allows us to establish tighter bounds on the unassisted capacity than were possible by direct considerations. To what extent this approach can be used in general, the reason such an approach works at all, and the tightness of the bounds achieved in this way are all questions that we leave wide open.

ACKNOWLEDGMENTS

It is a pleasure to thank Andrew Childs, Mary-Beth Ruskai, and Frank Verstraete for illuminating conversations about degradable channels and symmetric assistance.

BIOGRAPHIES

Graeme Smith received the B.Sc. degree in physics from the University of Toronto, Toronto, ON, Canada, in 2001 and the M.S. and Ph.D. degrees in physics from the California Institute of Technology, Pasadena in 2004 and 2006, respectively.

He is currently a Postdoctoral Fellow at the IBM T.J. Watson Research Center, Yorktown Heights, NY, working on quantum information theory, coding theory, and cryptography.

John A. Smolin received the S.B. degree in physics from the Massachusetts Institute of Technology (MIT), Cambridge, in 1989 and the Ph.D. degree, also in physics from the University of California, Los Angeles, in 1996.

After receiving the Ph.D. degree, he has been at IBM T.J. Watson Research Center, Yorktown Heights, NY, first and a postdoc and subsequently as a Research Staff Member. He, together with Charles Bennett built the first quantum cryptography apparatus at IBM in 1989. His current research interests are in quantum information theory, coding theory, and quantum computation, with the occasional misguided foray into the foundations of quantum mechanics.

Andreas Winter was born in Muhldorf am Inn, Germany in 1971. He received the Diploma degree in mathematics from the Freie Universitat Berlin, Berlin, Germany, in 1997. In 1999 he received the Ph.D. degree from the Fakultat fur Mathematik, Universitat Bielefeld, Bielefeld, Germany.

He was a Research Assistant at the University of Bielefeld until 2001, and since there has been with the University of Bristol, Bristol, U.K., most recently as Professor of Mathematics. His research interests include quantum information theory, complexity theory, and discrete mathematics. He is currently Associate Editor for Quantum Information Theory for the IEEE Transactions on Information Theory.

REFERENCES

- [1] C. E. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J.*, vol. 27, pp. 379–423 and 623–656, 1948.
- [2] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. Wiley & Sons, 1991.
- [3] S. Lloyd, "Capacity of the noisy quantum channel," *Phys. Rev. A*, vol. 55, pp. 1613–1622, 1997.
- [4] P. W. Shor, "The quantum channel capacity and coherent information," lecture notes, MSRI Workshop on Quantum Computation, 2002. Available online at <http://www.msri.org/publications/ln/msri/2002/quantumcrypto/shor/1/>.
- [5] I. Devetak, "The private classical capacity and quantum capacity of a quantum channel," *IEEE Trans. Inf. Theory*, vol. 51, pp. 44–55, 2005, arXiv:quant-ph/0304127.
- [6] V. Giovannetti and R. Fazio, "Information-capacity description of spin-chain correlations," *Phys. Rev. A*, vol. 71, p. 032314, 2005, arXiv:quant-ph/0405110.

- [7] E. M. Rains, “Bound on distillable entanglement,” *Phys. Rev. A*, vol. 60, pp. 179–184, 1999.
- [8] C. H. Bennett, D. P. DiVincenzo, and J. A. Smolin, “Capacities of quantum erasure channels,” *Phys. Rev. Lett.*, vol. 78, no. 16, pp. 3217–3220, Apr 1997.
- [9] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal, “Entanglement-assisted capacity of a quantum channel and the reverse Shannon theorem,” *IEEE Trans. Inf. Theory*, vol. 48, pp. 2637–2655, 2002.
- [10] C. Adami and N. Cerf, “von Neumann capacity of noisy quantum channels,” *Phys. Rev. A*, pp. 3470–3483, 1997.
- [11] J. A. Smolin, F. Verstraete, and A. Winter, “Entanglement of assistance and multipartite state distillation,” *Phys. Rev. A*, vol. 72, p. 052317, 2005, arXiv:quant-ph/0505038.
- [12] A. Winter, “On environment-assisted capacities of quantum channels,” arXiv:quant-ph/0507045.
- [13] B. Schumacher and M. A. Nielsen, “Quantum data processing and error correction,” *Phys. Rev. A*, vol. 54, p. 2629, 1996.
- [14] D. DiVincenzo, P. W. Shor, and J. A. Smolin, “Quantum channel capacity of very noisy channels,” *Phys. Rev. A*, vol. 57, no. 2, pp. 830–839, 1998, arXiv:quant-ph/9706061.
- [15] P. W. Shor and J. A. Smolin, “Quantum error-correcting codes need not completely reveal the error syndrome,” 1996, arXiv:quant-ph/9604006.
- [16] G. Smith and J. A. Smolin, “Degenerate quantum codes for Pauli channels,” *Phys. Rev. Lett.*, vol. 98, p. 030501, 2007, arXiv:quant-ph/0604107.
- [17] D. Bruss, D. P. DiVincenzo, A. Ekert, C. A. Fuchs, C. Macchiavello, and J. A. Smolin, “Optimal universal and state-dependent quantum cloning,” *Phys. Rev. A*, vol. 57, p. 2368, 1998, arXiv:quant-ph/9705038.
- [18] N. J. Cerf, “Quantum cloning and the capacity of the Pauli channel,” *Phys. Rev. Lett.*, vol. 84, p. 4497, 2000.
- [19] E. M. Rains, “A Semidefinite Program for Distillable Entanglement,” *IEEE Trans. Inf. Theory*, vol. 47, no. 7, pp. 2921–2933, 2001.
- [20] V. Vedral and M. B. Plenio, *Phys. Rev. A*, vol. 57, p. 1619, 1998, arXiv:quant-ph/9707035.
- [21] H. Barnum, E. Knill, and M. A. Nielsen, “On quantum fidelities and channel capacities,” *IEEE Trans. Inf. Theory*, vol. 46, pp. 1317–1329, 2000.
- [22] I. Devetak and P. W. Shor, “The capacity of a quantum channel for simultaneous transmission of classical and quantum information,” *Commun. Math. Phys.*, vol. 256, pp. 287–303, 2005, arXiv:quant-ph/0311131.
- [23] C. H. Bennett, A. W. Harrow, D. W. Leung, and J. A. Smolin, “On the capacities of bipartite Hamiltonians and unitary gates,” *IEEE Trans. Inf. Theory*, vol. 49, pp. 1895–1911, 2003, arXiv:quant-ph/0205057.
- [24] M. Christandl and A. Winter, “‘squashed entanglement’: An additive entanglement measure,” *J. Math. Phys.*, vol. 45, no. 3, pp. 829–840, 2004, arXiv:quant-ph/0308088.
- [25] C. A. Fuchs and J. van de Graaf, “Cryptographic distinguishability measures for quantum mechanical states,” *IEEE Trans. Inf. Theory*, vol. 45, pp. 1216–1227, 1999.
- [26] W. F. Stinespring, “Positive Functions on C^* -Algebras,” *Proc. Amer. Math. Soc.*, vol. 6, pp. 211–216, 1955.
- [27] E. H. Lieb and M.-B. Ruskai, “Proof of the strong subadditivity of quantum-mechanical entropy,” *J. Math. Phys.*, vol. 14, no. 12, pp. 1938–1941, 1973.
- [28] H. N. Barnum, M. A. Nielsen, and B. Schumacher, “Information transmission through a noisy quantum channel,” *Phys. Rev. A*, vol. 57, no. 6, pp. 4153–4175, 1998, arXiv:quant-ph/9702049.
- [29] M. Fannes, “A continuity property of the entropy density of spin lattice systems,” *Commun. Math. Phys.*, vol. 31, pp. 291–294.
- [30] G. Lindblad, “Completely positive maps and entropy inequalities,” *Commun. Math. Phys.*, vol. 40, pp. 147–151, 1975.
- [31] P. W. Shor, J. A. Smolin, and B. M. Terhal, “Nonadditivity of Bipartite Distillable Entanglement Follows from a Conjecture on Bound Entangled Werner States,” *Phys. Rev. Lett.*, vol. 86, pp. 2681–2684, 2000.
- [32] D. P. DiVincenzo, P. W. Shor, J. A. Smolin, B. M. Terhal, and A. V. Thapliyal, “Evidence for bound entangled states with negative partial transpose,” *Phys. Rev. A*, vol. 61, p. 062312, 2000.
- [33] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, “Mixed state entanglement and quantum error correction,” *Phys. Rev. A*, vol. 54, pp. 3824–3851, 1996, arXiv:quant-ph/9604024.
- [34] B. Kraus, N. Gisin, and R. Renner, “Lower and upper bounds on the secret key rate for quantum key distribution protocols using one-way classical communication,” *Phys. Rev. Lett.*, vol. 95, p. 080501, 2005, arXiv:quant-ph/0410215.
- [35] R. Renner, N. Gisin, and B. Kraus, “Information-theoretic security proof for quantum-key-distribution protocols,” *Phys. Rev. A*, vol. 72, p. 012332, 2005, arXiv:quant-ph/0502064.